What is claimed is:

1. An access control system comprising:

a memory which stores necessary information for various processes;

a processor for input/output to a file stored in a storage medium;

a policy file in said memory in which access control policy for said file is described;

an access controller which determines the validity of a request for access to said file according to said access control policy;

a monitoring processor which monitors issuance of a file access request made by means of said input/output processor, notifies said access controller of an issued file access request and receives the result of validity determination from said access controller; and

an exclusive controller which protects said memory's storage regions in use by said input/output controller, access controller and monitoring processor and shields said policy file from an access execution processor other than said input/output controller, access controller and monitoring processor, wherein:

said policy file contains information as an access control policy to identify the access request source, access execution processor and access type for the file to be accessed; and

said monitoring processor uses information to identify the access request source, access execution processor and access type to notify said access controller of said issued file access request.

2. The access control system as defined in claim 1, wherein said access control policy comprises information on an access type prohibited for access to said file, an error code which is returned to the access request source if said prohibited type of access occurs, and information to identify the access execution processor and access request source which are authorized by exception to access the file.

3. The access control system as defined in claim 2, wherein the access execution processor described in said access control policy is a program and is identified by a combination of the program's pathname and feature value.

4. The access control system as defined in claim 3, said system having an access log file which registers the content of a file access request, wherein

said access controller checks said file access request against the description of said policy file and transmits the result of said validity determination to said monitoring processor; and

if said access request is authorized, transmits the feature value of said access execution processor to said monitoring processor; or

if said access request is contrary to said access control policy, registers the content of said file access request in said access log file.

5. The access control system as defined in claim 4, wherein the system also incorporates an open file table as well as a processor that, if the access type of a valid file access request is an open access, registers, in said open file table, the access type, the file to be accessed and the access request source, and information to identify the access execution processor, which are obtained as response information from said access controller; and a processor that, if said access request is a read or write request, searches said open file table and determines the validity of said access request.

6. The access control system as defined in claim 5, wherein said monitoring processor also has a processor that, upon detecting a read or write access request not registered in said open file table, registers the content of said access request in said access log file through said access controller.

7. The access control system as defined in claim 6, wherein said monitoring processor also has a processor that, upon detecting a file close request, deletes the corresponding information from said open file table.

8. The access control system as defined in claim 4, wherein said access controller performs said check of the access request attribute information against the description in the policy file if the access type of said file access request is an open access and the attribute information for the file access request includes information on read access or write access.

9. The access control system as defined in claim 8, wherein said monitoring processor also has a processor that, if said file access request is valid, calculates the feature value for said access execution processor and compares it with the feature value received from said access controller; and

a processor that, if the values are the same, authorizes said access request; and

a processor that, if the values are not the same, invalidates said file access request and registers the content of the file access in said access log file through said access controller.

10. An information processing system comprising:

a first OS for controlling a processor for input/output to files and a first memory processor for exclusive use; a second OS for controlling a second memory processor for exclusive use; and a communication processor for data communications between said first OS and second OS, wherein said first OS has a monitoring processor to monitor a file access request issued to said processor for input/output to files under its control;

said second OS has an access controller to determine the validity of said file access request according to the access control policy; and

said monitoring processor notifies said access controller of said access request through said communication processor and receives the result of validity determination from said access controller through said communication processor.

11. The information processing system as defined in claim 10, wherein said second OS has a policy file which contains information as said access control policy to identify the access request source, access execution processor and access type.

12. The information processing system as defined in claim 11, wherein the access execution processor described in said access control policy is a program and is identified by a combination of the program's pathname and feature value.

13. The information processing system as defined in claim 12, said second OS also having an access log file which registers the content of a file access request, wherein said access controller checks said file access request against the

description of said policy file and transmits the result of validity determination to said monitoring processor and, if said access request is authorized, transmits the feature value of said access execution processor to said monitoring processor, or if said access request is contrary to said access control policy, registers the content of said file access request in said access log file.

14. The information processing system as defined in claim 13, wherein said first OS also incorporates an open file table as well as a processor that, if the access type of a valid file access request is an open access, registers in said open file table, the access type, the file to be accessed, the access request source and information to identify the access execution processor, all of which have been obtained as response information from said access controller; and a processor that, if a read or write access request is issued as said access request, searches said open file table and determines the validity of said access request.

15. The information processing system as defined in claim 14, wherein said monitoring processor also has a processor that, if it detects a read or write access request not registered in said open file table, registers the content of said access request in said access log file through said access controller.

16. The information processing system as defined in claim 15, wherein said monitoring processor also has a processor that, if it detects a file close request, deletes the corresponding information from said open file table.

17. The information processing system as defined in claim 13, wherein said access controller performs said check of the attribute information against said policy file description if the access type of said file access request is an open access and the attribute information for the file access request includes information on read access or write access.

18. The information processing system as defined in claim 17, wherein said monitoring processor also has a processor that, if said file access request is determined to be valid, calculates the feature value for said access execution processor and compares it with said feature value received from said access controller;

a processor that, if the values are the same, authorizes said access request; and

a processor that, if the values are not the same, invalidates said file access request and registers the content of the file access in said access log file through said access controller.

19. An access control system for use with an information processing system comprising:

a first OS for controlling a processor for input/output to files and a first memory processor for exclusive use;

a second OS for controlling an second memory processor for exclusive use; and

a communication processor for data communications between said first OS and second OS, wherein the information processing system has a monitoring processor which monitors a file access request issued to said processor for input/output to files which is incorporated in and controlled by said first OS; and

an access controller, under the control of said second OS, which determines the validity of said file access request according to the access control policy, and wherein said monitoring processor notifies said access controller of said access request through said communication processor and receives the result of validity determination from said access controller through said communication processor.

20. A program product comprising programs which are loaded and executed in an information processing unit provided with a processor for input/output to files and a memory for storing said files and constitute an access control system on said information processing unit, and files which are used by said programs, the product having the following:

a policy file in which an access control policy is described; an access control program, a monitoring program; and a computer-readable medium to embody said programs; wherein said access control policy contains information to identify the access request source, access execution processor and access type for the file to be accessed; and said access control program has codes to enable said information processing unit to determine the validity of the file access request according to said access control policy; and said monitoring program has codes to enable said information processing unit to monitor issuance of a file access request made by means of said input/output processor as well as codes to enable said information processing unit to notify said access control program of the issued file access request using the information to identify the access request source, access execution processor and access type.